УДК 341.48/.49

М. Ю. ЯЦИШИН

«ІНТЕРНЕТ РЕЧЕЙ» В СИСТЕМІ МІЖНАРОДНО-ПРАВОВОЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Досліджується проблема міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю в контексті впровадження новітніх технологій. Аналіз здійснюється на прикладі Інтернету речей (Internet of Things), що уже отримав значне поширення у світі. Автор відзначає відсутність загальновизнаного понятійно-категоріального апарату, а також універсального міжнародного договору у сфері боротьби з кіберзлочинністю. Встановлено, що інновації можуть використовуватись злочинцями як засоби вчинення протиправних діянь або об'єкти злочинних посягань. В результаті дослідження чинних регіональних актів автор приходить до висновку, що сфера їх дії в цілому охоплює нові технічні досягнення, однак спеціальне нормативне регулювання відсутнє. Автор пропонує з метою підвищення ефективності міжнародно-правового співробітництва у боротьбі з кіберзлочинністю включення до міжнародних угод положень про «емерджентні технології».

Ключові слова: *кіберзлочинність, кібербезпека, Інтернет речей, міжнародне право, емерджентна технологія.*

Яцишин М. Ю. **«Интернет вещей» в системе международно-правового противодействия киберпреступности**

Исследуется проблема международно-правового сотрудничества государств в борьбе с киберпреступностью в контексте внедрения новых технологий. Анализ осуществляется на примере Интернета вещей (Internet of Things), который уже достаточно распространён в мире. Автор отмечает отсутствие общепринятого понятийно-категориального аппарата, а также универсального международного договора в сфере борьбы с киберпреступностью. Установлено, что инновации могут использоваться преступниками в качестве средств для совершения преступных деяний или объекта преступного посягательства. На основании исследования действующих региональных актов автор приходит к выводу, что сфера их действия в целом охватывает новые технические достижения, но специальное право-

---

© *ЯЦИШИН Марта Юріївна* – старший викладач кафедри міжнародного права Навчально-наукового інституту міжнародних відносин Національного авіаційного університету

вое регулирование отсутствует. Автор предлагает с целью повышения эффективности международно-правового сотрудничества в борьбе с киберпреступностью дополнить международные соглашения положениями об «эмерджентных технологиях».

Ключевые слова: *киберпреступность, кибербезопасность, Интернет вещей, международное право, эмерджентная технология.*

Yatsyshyn Marta. **«Internet of Things» in the International Legal System against Cybercrime**

This article deals with the problem of international legal cooperation in fight cybercrime in the context of new technologies introduction. The analysis is carried out on an example of the Internet of things that has already spread in the world. The author notes the absence of a general terminology, as well as a universal international agreement in the field of cybercrime resistance. It has been established that criminals can use innovations as means of unlawful actions or objects of criminal encroachment. Because of the study, the author concludes that reginal acts generally covers new technical achievements, but there is no specific regulation. The author proposes the inclusion of provisions on «emerging technologies» in the international agreements, with the aim of increasing the effectiveness of international legal cooperation against cybercrime.

Keywords: *cybercrime, cybersecurity, Internet of things, International Law, Emerging Technology.*

Кіберзлочинність є явищем динамічним, що змінюється, удосконалюється та отримує все більше поширення. Як зазначив на спільній конференції Інтерполу та Європолу Стівен Вільсон (Steven Wilson), голова Європейського центру з кіберзлочинності (European Cybercrime Centre): «2018 рік визначний щодо успішності правозастосування у боротьбі з кіберзлочинністю на глобальному рівні, він також підвищив публічне усвідомлення ризиків, однак кіберзлочинці стають розумнішими і більш цілеспрямованими у своїй діяльності, представляючи собою постійно зростаючу загрозу»[1]. Тому міжнародне співробітництво держав у боротьбі з кіберзлочинністю також повинно динамічно реагувати на такі зміни.

У процесі вдосконалення матеріально-правової протидії кіберзлочинності важливо враховувати тенденції розвитку останньої. Так, багато дослідників відзначають, що високотехнологічна злочинність у майбутньому буде пов'язана з такими

новаціями, як штучний інтелект (Artificial intelligence), хмарні технології (Cloud Technology), Датагрід (Data grid), технології розподілених баз даних (Distributed Ledger Technology, далі – DLT), Блокчейн (Block chain) та Інтернет речей (Internet of Things, далі – IoT). Впровадження і широке використання цих технічних досягнень здійснює значний вплив на суспільні відносини, а тому потребує додаткового правового регулювання[2]. З іншої сторони, виникають нові можливості, що можуть бути використані правопорушниками для здійснення кіберзлочинів, негативні наслідки яких постійно масштабуються.

Крім цього, слід врахувати, що інформаційні технології розвиваються дуже стрімкими темпами. Тому постає важлива наукова проблема, як теоретичного, так і практичного спрямування, щодо визначення можливостей сучасних норм міжнародного права виконувати прогностичну функцію, засуджувати і попереджувати майбутні види і схеми кіберзлочинності. З цією метою важливим є дослідження місця новітніх технологій в існуючій системі міжнародно-правового регулювання боротьби з кібернетичними злочинами, яке ми проведемо на прикладі «Інтернету речей».

Міжнародно-правова протидія кіберзлочинності є достатньо новим напрямком наукових досліджень. Серед вітчизняних та зарубіжних авторів, що здійснювали аналіз цієї проблематики слід виділити А. В. Пазюка, І. М. Забару, О. О. Мережко, а також Дж. Блумбекера (J. Bloombecker), Ш. Шольберга (S. Schjolberg), У. Зібера (U. Sieber), Д. Вол (D. Wall) та М. Яр (M. Yar). Однак, у своїх дослідженнях автори не розглядали сучасні тенденції удосконалення техніки, зокрема Інтернету речей, в рамках системи міжнародно-правового співробітництва держав щодо боротьби з кіберзлочинністю.

Особливо важливими у визначеній сфері є напрацювання Науково-дослідного інституту інформатики і права Національної академії правових наук України, зокрема монографії О. Д. Довгань та І. М. Доронін «Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки»[3], а також О. А. Баранова «Інтернет речей: теоретико

методологічні основи правового регулювання»[4]. В своїх працях автори здійснили ґрунтовний аналіз правового регулювання Інтернету речей згідно чинного законодавства України. Проте, дослідження регулювання новітніх технологій в рамках інституту міжнародно-правової протидії кіберзлочинності залишаються актуальними.

Отже, метою цієї статті є визначення та комплексний аналіз місця інноваційних технологій в системі міжнародно-правової боротьби з кіберзлочинністю на прикладі Інтернету речей. Її новизна полягає у новому підході до розуміння сфери дії міжнародних договорів про високотехнологічну злочинність, що повинен бути врахованим при формуванні універсальної концепції кіберзлочинності та розробці Конвенції ООН у визначеній сфері. Завдання статті полягають визначенні основних понять (кіберзлочинності та Інтернету речей) та їх взаємозв'язків, дослідження сфери дії чинних міжнародно-правових актів про кібернетичну злочинність в контексті використання технології Інтернету речей, а також формування на основі проведеного аналізу узагальненого підходу щодо удосконалення матеріальних норм інституту міжнародної протидії кіберзлочинності.

Перш за все, необхідно зазначити, що єдине загальноприйняте юридичне визначення поняття «Інтернет речей» відсутнє. Повністю підтримуємо підхід, запропонований професором О. Барановим, що надає наступну дефініцію: «Інтернет речей – це сукупність взаємодіючих технічних систем і комплексів, призначених для реалізації суспільних відносин, у тому числі, пов'язаних з наданням послуг або проведенням робіт, на основі використання різноманітних даних і мережі Інтернет за безпосередньої участі або без участі суб'єктів цих відносин (юридичних чи фізичних осіб)»[5]. В рекомендації ITU надано наступне визначення Інтернету речей – глобальна інфраструктура для інформаційного суспільства, яка дозволяє отримувати (надавати) сучасні послуги за допомогою з'єднання (фізичного і віртуального) речей, заснованих на існуючих і тих, які будуть розроблятись, сумісних інформаційних і комунікаційних технологіях[6].

У дослідженні Інституту Інтернету речей (Internet of Things Institute, США) серед потенційних загроз використання комерційних безпілотних літальних апаратів (БПЛА) визначається їх використання з протиправною метою (зокрема, для контрабанди, постачання наркотиків, передачі заборонених об'єктів тощо)[7]. Під загрозами негативного неправомірного впливу перебувають й інші об'єкти, серед яких безпілотні пристрої наземного транспорту та об'єкти критичної інфраструктури[8]. Як стверджує Д. Вест (D. West), проектування сучасних об'єктів Інтернету речей, зокрема безпілотних автомобілів, відбувалось з урахуванням можливостей перехоплення управління ними та вимог кібербезпеки[9].

За прогнозами Gartner до 2020 року загальна кількість засобів, підключених до мережі Інтернет, не враховуючи персональні комп'ютери, планшети та смартфони буде нараховувати 26 млн одиниць[10]. Відповідно до інформації, оприлюдненої дослідниками компанії Proofpoint, у 2014 році протягом 2 тижнів більше 100 тис. смарт-телевізорів, холодильників та інших споживчих приладів використовувались хакерами для пересилання шкідливих електронних листів[11]. Важливо зазначити, що пристрої IoT застосовуються не лише для побутових цілей, а й для обслуговування виробничих процесів, населених пунктів, житла і будівель (smart міста та квартири), а також об'єктів критичної інфраструктури. Професор Кріс Хенкін (Chris Hankin), відзначає серед іншого такі проблеми приладів IoT, як їхнє створення на основі дешевого чи неякісного апаратного і програмного забезпечення, а як результат – наявність вразливостей[12]. Отже пристрої, які складають в загальному поняття «Інтернету речей», можуть потенційно бути, з однієї сторони, засобами, за допомогою яких здійснюються кіберзлочини, а з іншої – матеріальними об'єктами такого протиправного посягання.

Виклики для кібербезпеки пов'язані із впровадженням IoT розглядались в рамках третьої (10-13.04.2017 р.) та четвертої наради (03-05.04.2018 р.) міжурядової групи експертів відкритого складу, створеної на підставі Резолюції 65/230 ГА ООН у

2010 році відповідно до пункту 42 Сальвадорської декларації про комплексні стратегії для відповіді на глобальні виклики: системи попередження злочинності та кримінального правосуддя і їхній розвиток в світі, що змінюється. Рішення групи експертів ООН представляють собою компіляції думок і підходів, не відображають міждержавного консенсусу і не мають обов'язкової юридичної сили. Однак, вони є корисним довідковим матеріалом, що носить рекомендаційний характер. Так, експертами було відзначено необхідність активізувати співпрацю держав, зокрема, в сфері використання Інтернету речей[13].

Характеризуючи сучасний стан боротьби з кібернетичними злочинами правомірним буде ствердження, що ця система уже вийшла за рамки національних правових засобів, однак ще не інтегрована до системи міжнародного кримінального права. Ст. 5 Статуту Міжнародного суду ООН не передбачає відповідальності за кіберзлочинність, а отже такого злочину за міжнародним правом не існує. Універсальний міжнародний договір про кіберзлочинність також відсутній, регіональні договори неузгоджені між собою, що призводить до значної фрагментації та неоднорідності міжнародно-правового регулювання визначеної сфери.

Проте, сьогодні об'єктивно існує сукупність міжнародно-правових норм різного рівня та спрямування, що складає нормативну основу інституту міжнародно-правової протидії кіберзлочинності, який перебуває на стадії формального становлення. Так, міжнародна співпраця держав у боротьбі з кібернетичними злочинами відбувається на наступних рівнях: 1) В рамках ООН та її спеціалізованих установ (МСЕ, Інтерпол та ін.); 2) На основі регіональних угод, зокрема (РЄ, ЛАД, ШОС, АС, СНД та ін.); 3) Відповідно до двосторонніх договорів про надання правової допомоги з кримінальних питань, видачі злочинців, професійно-технічну допомогу, розслідування кіберінцидентів, збирання і передачу доказів тощо; 4) За допомогою неформальних каналів (співпраця правоохоронних органів, служб, агентств, відомств).

Основними міжнародними договорами, що мають обов'язкову силу для держав учасниць в сфері протидії кіберзлочинності є: Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р.; . Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р.; Угода про співробітництво держав – членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01.06.2001 р.; Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. та Конвенція про кібербезпеку і захист персональних даних Африканського Союзу 27.06.2014 р. Положення ст. 1 Конвенції про кіберзлочинність Ради Європи міститься поняття «комп'ютерної системи», що відповідно до офіційного тлумаченням Комітету (Cybercrime Convention Committee – T-CY) наданого у 2012 році, включає різного роду гаджети, які здійснюють обробку «комп'ютерних даних», а також створюють «дані про рух інформації»[14]. Фактично, подібні підходи закріплені в Конвенції Ліги арабських держав, що застосовує поняття «інформаційної технології»[15], Угоді Шанхайської організації співробітництва, яка містить термін «інформаційна інфраструктура»[16] та Конвенція Африканського союзу, в якій використовується поняття «комп'ютерна система»[17]. Що стосується Угоди Співдружності незалежних держав, то в чинній редакції 2001 р. закріплено поняття «комп'ютерної інформації» як інформації, що знаходиться в пам'яті комп'ютера, на машинних чи інших носіях в формі, доступній сприйняттю ЕОМ, або передається каналами зв'язку[18]. Редакцією 2017 р., яка вже відкрита для підписання, але не набула чинності, змінено термінологію і використовується також поняття «інформаційних технологій», що повністю відповідає іншим регіональним актам.

Як зазначається Глобальною комісією з управління Інтернету, для IoT притаманні три ознаки: по-перше, підключення до Інтернету (незалежно чи окремого пристрою, чи базової станції); по-друге, наявність цифрового сенсору, що

збирає вхідні дані; і по-третє, наявність процесору[19]. Загалом, існують два види даних в рамках IoT: 1) дані, створені кінцевими вузлами інфраструктури, як наприклад датчиками, що збирають інформацію із оточуючого середовища; 2) дані, що передаються через IoT. Елементи систем IoT можуть збирати чи синтезувати мільярди бітів даних, створюючи при цьому цінні відомості. Отже, таким чином усі пристрої Інтернету речей підпадають під дію чинних регіональних угод в сфері боротьби з кіберзлочинністю (за виключенням Конвенції СНД 2001 р.).

Таким чином, саме завдяки принципу технічної нейтральності (Technological Neutrality Principle) сфера дії норм міжнародного права в сфері протидії високотехнологічній злочинності може постійно розширюватись і включати новостворені технології. Цей принцип вперше був застосований в США[20] у 1997 році, а потім в Директиві Єврокомісії (Directive 2009/140/ЕС) у 1999 році щодо електронних комунікацій[21]. Згодом підтверджувався в Окінавській хартії глобального інформаційного суспільства та Всесвітньому Саміті ООН з Інформаційного суспільства (WSIS). У сфері регулювання ІКТ цей принцип забезпечує еквівалентну оцінку технологій, оскільки забороняє надавати будь-якій з них пріоритет над іншим. Як результат, це допомагає уникати обмежень застосування законодавства, які виникають у зв'язку з використанням конкретних термінів, пов'язаних із технологіями.

Існує думка, що даний принцип не відповідає вимогам повноти, точності і чіткості визначення злочину[22]. Однак, ми повністю підтримуємо точку зору В. Максвелла (W. Maxwell), що в сфері кібербезпеки відступ від принципу технологічної нейтральності призведе до більшої шкоди, аніж користі, оскільки у такому випадку регулювання буде структуровано в залежності від конкретних технологій[23]. Тому, законодавство має абстрагуватися від технологій у тій мірі, в якій воно забезпечує достатню правову визначеність. Достатній рівень конкретизації при загальній нейтральності технічної термінології, зокрема може досягатись за допомогою прийняття додаткових пояснень, що періодично оцінюються і переглядаються. Це також

означає, що для регулювання сфери протидії кіберзлочинності прийняття лише конвенційних без паралельних інституційних механізмів не є достатнім. Позитивне значення технічної нейтральності, а як наслідок і достатня гнучкість норм Конвенції РЄ, відзначалась в оді третьої та четвертої наради групи експертів ООН.

Слід зазначити, що на основі принципу технічної нейтральності формується важливе положення про взаємне визнання злочину при відсутності необхідності дотримуватись єдиної термінології за умов, що відповідне діяння визнається злочинним у всіх правових системах. Саме завдяки такому підходу відбувається зближення і гармонізація національних кримінальних законодавств. З іншої сторони, завдяки взаємному визнанню кіберзлочинів, міжнародне співтовариство обмежує можливість створення «цифрових притулків» для правопорушників (тобто таких правопорядків, де злочинці б уникали відповідальності).

Автори монографії «Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту», О. Д. Довгань, І. М. Доронін, пропонують впровадження терміну «емерджентної технології», що означає технологію, яка є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед[24]. Включення до міжнародно-правових актів положень щодо протидії кіберзлочинності в рамках «емерджентних технологій» значно посилило би регулювання визначеної сфери.

Отже, в процесі проведеного дослідження приходимо до наступних висновків. В системі міжнародно-правової протидії кіберзлочинності не передбачено спеціального регулювання для Інтернету речей. IoT разом із іншими ІКТ виступає в якості засобу здійснення високотехнологічної злочинності, або об'єкту злочинних посягань. Вирішення проблеми фрагментарності і неоднорідності досліджуваного інституту, на нашу думку, полягає в створенні та прийнятті в рамках ООН міжнародного

договору про кіберзлочинність. В його основу повинна бути покладена універсальна концепція кіберзлочинності, розроблена відповідно до чинних принципів і норм міжнародного права, а також чинних регіональних актів, що набули поширення, в першу чергу Конвенції Ради Європи, а також найкращої світової практики.

Запропонована універсальна концепція кіберзлочинності повинна поширювати свою дію не лише на існуючі технології, а й здійснюючи прогностичну функцію, попереджати використання інноваційних технологій у здійсненні злочинних діянь. Тому положення майбутньої Конвенції ООН про кіберзлочинність повинні відповідати принципові технічної нейтральності, з однієї сторони, а з іншої – включати положення про розширення сфери дії на «емерджентні технології». Це твердження повинно бути формалізованим у загальну норму, що додатково буде тлумачитись спеціально визначеним органом, на кшталт Комітету T-CY відповідно до Конвенції про кіберзлочинність Ради Європи.

1. *Interpol-Europol* conference calls for global response to cybercrime // Interpol.int. URL: https://www.interpol.int/News-and-media/News/2018/N2018-096 **2.** *Довгань О. Д., Доронін І. М.* Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту. Київ: Видавничий дім «АртЕк», 2017. С. 45. **3.** Там само. **4.** *Баранов О. А.* Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія. Київ: Видавничий дім «АртЕк», 2018. 344 с. **5.** *Баранов О.* «Інтернет речей» як правовий термін // Юридична Україна. URL: http://nbuv.gov.ua/UJRN/urykr_2016_5-6_16 **6.** *Recommendation* Y.4000/Y.2060 (06/12) // Information and Telecommunication Union. URL : https://www.itu.int/rec/T-REC-Y.2060-201206-I **7.** *Buntz B.* 10 of the Top Drone Security Worries // IOT Institute Revue. URL: http://www.ioti.com/security/10-top-drone-security-worries **8.** *Simon T.* Critical Infrastructure and the Internet Of Things // Global Commission on Internet Governance. URL: https://www.cigionline.org/sites/default/files/ documents/GCIG%20no.46_0.pdf **9.** *West D.* Moving Forward: Self-Driving vehicles in China, Europe, Japan, Korea and the United States // Center for Technology Innovation at Brookings Institute. URL: https://www.brookings. edu/wp-content/uploads/2016/09/driverless-cars-2.pdf **10.** *Gartner Says* the

Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 // Gartner. URL: https://www.gartner.com/newsroom/id/2636073 **11.** *IoT* – Discovered first Internet of Things cyberattack on large-scale. URL: https://securityaffairs.co/wordpress/21397/cyber-crime/iot-cyberattack-large-scale.html **12.** *The Internet* of Things: opportunities and threats. Conference report URL: https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf **13.** *Доклад* о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 3-5 апреля 2018 года. URL: http://www.unodc.org/documents/organized-crime/cybercrime/ cybercrime-april-2018/V1802317.pdf **14.** *T-CY* Guidance Note #1. On the notion of computer system Article 1.a Budapest Convention on Cybercrime. URL: https://rm.coe.int/CoERMPublicCommonSearch Services/DisplayDCTMC ontent?documentId=09000016802e79e6 **15.** *Arab* Convention on Combating Technology Offences of 21.12.2010. URL: https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd **16.** *Соглашение* между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement Russian.pdf **17.** *African* Union Convention on Cyber Security and Personal Data Protection of 27.06.2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_ e.pdf **18.** *Соглашение* о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001. URL: http://base.garant.ru/12123778/ **19.** *Critical* Infrastructure and the Internet of Things. URL: https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0 **20.** *Chris* Reed Taking Sides on Technology Neutrality. URL: https://www.researchgate.net/publication/265280565_Taking_Sides_on_Technology_Neutrality **21.** *Directive* 2009/140/EC of the European Parliament and of the Council of 25.11.2009. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L: 2009:337:0037: 0069:EN:PDF **22.** *The Technological* Neutrality Principle and Its Significance in Formulating and Explaining the Offences Against the Security of Electronic Data and Information Systems. URL: https://www3.mruni.eu/ojs/societal-studies/article/view/249 **23.** *W. Maxwell.* Technology neutrality in Internet, telecoms and data protection regulation. URL: https://www.hlmediacomms.com/2014/11/17/technology-neutrality-in-internet-telecoms-and-data-protection-regulation/ **24.** *Довгань О. Д., Доронін І. М.* Цит. праця. С. 66.

***Yatsyshyn Marta*. «Internet of Things» in the International Legal System on Combating Cybercrime**

Cybercrime is a very dynamic phenomenon, which become more complicated and dangerous. That is why International cooperation in fight cybercrime have to take dynamic reaction. High-tech crime in the future will be associated with Artificial Intelligence, Cloud Technology, Data Grid, Distributed Ledger Technology, Block Chain and Internet of Things, New opportunities provided with these technologies can be widely used by criminals. This article outlines issues of prohibition innovations application to cybercrime under international law. The author use as an example Internet of things. The goal of this article is to identify and analyze the place of innovation technologies in international law system to combat cybercrime.

The author mentioned the term of Internet of Things and its main characteristics. There is no unified legal terminology in this field. The article established various international legal acts that mentioned Internet of Thing as an element of cybercrime. Internet of Things or other innovations could be used as a means of high-tech crime, or an object of criminal encroachment. In case of a universal convention of cybercrime absence, the author analyze main regional agreements adopted by the Council of Europe, League of Arab States, Commonwealth of Independent States, Shanghai Organization of Cooperation and African Union. Because of the study, it was established that all Internet of Things devises are under valid regional agreements regulation. Technological Neutrality Principle can extend the scope of international rules against cybercrime. In spite of this, there is no special regulatory rules for innovations in field of cybercrime counteraction.

In our opinion, solving the problem of fragmentation of the International legal system on Combating Cybercrime is the creation and adoption international agreement on cybercrime within the United Nations framework. It should be based on the universal concept of cybercrime, developed in accordance with the current principles and norms of international law, as well as the existing regional acts that have become widespread. The provisions of the future UN Convention on Cybercrime must comply with the principles of technical neutrality, on the one hand, and on the other – include provisions on extending the scope of «emerging technologies». This statement must be formalized into a general rule, which will additionally be interpreted by a specially designated body, such as the T-CY Committee, in accordance with the Council of Europe's Convention on Cybercrime.

Keywords: cybercrime, cybersecurity, Internet of things, International Law, Emerging Technology.